Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 8 March 2005 Meeting

GSA; 1800 F Street; Room 5141A; Washington, DC

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Discuss/Vote on Minutes for 14 December 2004, 11 January 2005, and 08 February 2005
3) Status of Email Votes Since Last FPKIPA Meeting
4) Federal Identity Credentialing Committee (FICC) Report
5) FPKI Certificate Policy Working Group (CPWG) Report
6) Federal PKI Operational Authority (FPKI OA) Report
7) Final Meeting Items
8) Meeting Adjourned / Next Meeting Plans

B. ATTENDANCE LIST

VOTING MEMBERS

Organization	Name	Email	Telephone
Dept of Commerce (NIST)	Polk, Tim		
Dept of Defense	Mitchell, Debbie		
Dept of Energy	ABSENT		
Dept of Health & Human Services	Alterman, Peter		
Dept of Justice	Morrison, Scott		
Dept of State	Cao, Tin		
Dept of the Treasury	ABSENT		
GSA	Cornell, John		
NASA	DeYoung, Tice		
OMB	ABSENT		
USDA/NFC	Sharp, Kathy		
USPTO	Purcell, Art		

OBSERVERS

Organization	Name	Email	Telephone
ACES	Duncan, Steve		
Dept of Energy	Izzo, Bill		
Dept of Health & Human Services	Fortwengler, George		
Dept of State (Mantech)	Froehlich, Charles R.		
EDUCAUSE	Worona, Steve		
FICC	Petrick, Brant		
FICC	Spencer, Judy		
FPKI OA Director (GSA)	Jenkins, Cheryl		
FPKI OA (Mitretek)	Stern, Michael		
FPKI OA (Mitretek)	Tate, Darron		
FPKIPA Secretary (IATAC)	Lentz, Mark		
State of Illinois	Anderson, Mark		
US Patent & Trademark Office (USPTO)	Rutherford, Chris		

C. MEETING ACTIVITY

Agenda Items 1 & 2

Introductions / Vote on Approval of Meeting Minutes
This meeting took place at the GSA Headquarters Building, 1800 F Street, Washington, DC in Room 5141A. Dr. Peter Alterman, Department of Health & Human Services (HHS) and FPKIPA Chair, called the meeting to order at 9:45 a.m. with attendee introductions.

The 14 December 2004 meeting minutes were recommended by motion for approval vote (NASA) and seconded (Dept of Sate). These minutes were unanimously approved by voice vote.

The 11 January 2005 meeting minutes were recommended by motion for approval vote (GSA) and seconded (NASA). These minutes were unanimously approved by voice vote.

The 08 February 2005 meeting minutes were recommended by motion for approval vote (GSA) and seconded (Defense). These minutes were unanimously approved by voice vote.

Agenda Item 3

Status of Email Votes Since Last FPKIPA Meeting
There were two items voted on via email votes since the last FPKIPA meeting on 8 February 2005. The email vote records for these items are attached as Appendix A of these minutes.

Mr. Mark Lentz, IATAC and the FPKIPA Secretary, provided a brief summary of the outcome of the email vote for each of the two items:

PTO Compliance Audit and Cross-Certification (Medium) - Compliance Audit was the only remaining cross-certification criteria for PTO to get approved, so this email vote was for both their compliance audit and cross-certification at the Medium assurance level. All 11 voting members voted Yes to approve both the PTO compliance audit and cross-certification at the Medium assurance level. As a result of this vote, this is the first FPKIPA meeting attended by PTO as a voting member.

State of Illinois Compliance Audit - All 11 voting members voted Yes to approve the State of Illinois compliance audit via the email vote. With the approval of their compliance audit, the State of Illinois has met all the criteria for cross-certification at the Basic assurance level. Therefore, the motion was made by GSA and seconded by NASA to approve the State of Illinois for cross-certification at the Basic Assurance level during this meeting. Here is the voting record:

Approval vote for State of Illinois Cross-Certification (Basic)			
Voting members	**Vote (Motion – GSA; 2nd – NASA)**		
	Yes	**No**	**Abstain**
Dept of Commerce (designated proxy – Peter Alterman)	X		
Dept of Defense	X		
Dept of Energy	ABSENT – did not vote		
Dept of Health & Human Services	X		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury	ABSENT – did not vote		
GSA	X		
NASA	X		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

Agenda Item 4

Federal Identity Credentialing Committee (FICC) Report
Ms. Judith Spencer, FICC, informed the attendees that FIPS 201 was signed and released on schedule at the end of February.

NIST Special Publication 800-73, the technical specification for Smart Cards, was scheduled to be released during the week of this meeting.

NIST Special Publication 800-76, the technical specification for Biometrics (defining fingerprint specifications only) was about to be released for public comment and should be released in its final form by the end of March.

NIST Special Publication 800-78, Recommendation for Cryptographic Algorithms and Key Sizes, will be released soon. In addition to the theoretical compromise of SHA-1, it is also important to note that the MD5 hash algorithm has been fully compromised (demonstrated), but SHA-1 has been more widely used than MD5, so that compromise is not seen as a major impact to the security product and services industry. NIST will be coming out with a statement regarding the compromises of MD5 and SHA-1 and what impact they will have on NIST's recommendation of when to transition to the use of SHA-256. The previous recommendation for transition to SHA-256 had been 2010.

ACTION (126): Ms. Cheryl Jenkins, GSA, will determine, using the Entrust CA product, how soon it will be practical to transition to the use of SHA-256.

Shared Service Providers (SSP) - ORC has submitted the appropriate paperwork for consideration as an SSP, so a meeting will be coordinated soon to discuss their application and approval as an SSP. AT&T and DST have not submitted their SSP application yet. The Social Security Administration (SSA) has expressed interest to Ms. Spencer to also be an SSP.

The GSA Technical Supplement, in support of OMB issued memorandum M-05-05, was released the week before this meeting to the CIO, CFO, and Chief Acquisition Officers of Federal agencies.

Agenda Item 5

FPKI Certificate Policy Working Group (CPWG) Report

Mr. Tim Polk, Department of Commerce (NIST) and CPWG Co-Chair, led the CPWG Report.

Department of Homeland Security (DHS) Compliance Audit
The CPWG had reviewed the DHS Compliance Audit Report at the 3 February meeting and determined that it contained all the appropriate audited events that are required for approval. The only aspect of the compliance audit that the CPWG still needed to see was the summary of the audit findings in a letter from the auditor using the auditor's letterhead paper. The CPWG obtained a letter from KPMG, the DHS auditor, and reviewed it at the 1 March CPWG meeting and found it to be sufficient. Therefore, the CPWG recommends the DHS Compliance Audit for FPKIPA approval.

The following table shows the voting record for the DHS Compliance Audit:

Approval vote for Department of Homeland Security (DHS) Compliance Audit			
Voting members	**Vote (Motion – GSA; 2nd – Justice)**		
	Yes	**No**	**Abstain**
Dept of Commerce	X		
Dept of Defense	X		
Dept of Energy	ABSENT – did not vote		
Dept of Health & Human Services	X		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury	ABSENT – did not vote		
GSA	X		
NASA	X		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

Common Policy Change Proposal, 2005-02

This change proposal was initiated from some of the FIPS 201 comments and facilitates the deployment of FIPS 201 compliant identity credentials, by adding the appropriate language to allow for cryptographic algorithms other than RSA. Elliptic Curve Cryptography (ECC) is particularly attractive when implemented on devices with limited power and computing capability. ECC is also easier to implement in hardware (due to smaller key sizes) and attacks that may work to compromise SHA-1 will not work against ECC algorithms.

The following table shows the voting record for the Common Policy Change Proposal, 2005-02:

Approval vote for Common Policy Change Proposal, 2005-02			
Voting members	**Vote (Motion – GSA; 2nd – NASA)**		
	Yes	**No**	**Abstain**
Dept of Commerce	X		
Dept of Defense	X		
Dept of Energy	ABSENT – did not vote		
Dept of Health & Human Services	X		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury	ABSENT – did not vote		
GSA	X		
NASA	X		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

The CPWG meeting schedule was announced, but location for each meeting is still to be determined:
1) 23 March – regular CPWG meeting

2) 5, 6 April – dedicated CPWG meeting to address outstanding FBCA CP comments and finalized RFC 3647 version of FBCA CP

3) 27 April – regular CPWG meeting

Agenda Item 9

Federal PKI Operational Authority (FPKI OA) Report

Status of CP/CPS Compliance Audit:

Ms. Cheryl Jenkins, FPKI OA Director, reviewed the status of the FPKIA CP/CPS Compliance Audit, stating the following highlights:

The FPKI OA met with their auditor, KPMG, the day before this meeting to discuss latest CPS changes made by the FPKI OA. KPMG agreed that the CPS changes made by the FPKI OA were sufficient. CP/CPS Audit is still on schedule with KPMG to be completed by the end of March 2005.

The RFC 2527 vs. RFC 3647 FBCA CP analysis is still on schedule and should be done by KPMG and delivered to the FPKI OA by 25 March 2005.

Technical Updates:

The FPKI OA will be sending information out to the FBCA cross-certification members regarding directory architecture updates for facilitating global searching.

Status of FBCA/Applicant Cross-Certification Technical Testing:

Government Printing Office (GPO) - technical testing is scheduled to start on 11 March.

Higher Education Bridge Certification Authority (HEBCA) – technical testing was completed with HEBCA on 4 February 2005. The FPKI OA distributed the report for HEBCA's testing prior to the meeting. Here is the voting record:

Approval vote for HEBCA Technical Testing			
Voting members	**Vote (Motion – NASA; 2nd – USPTO)**		
	Yes	**No**	**Abstain**
Dept of Commerce (designated proxy - FPKIPA Chair)	X		
Dept of Defense	X		
Dept of Energy	ABSENT – did not vote		
Dept of Health & Human Services	X		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury	ABSENT – did not vote		
GSA (designated proxy - FPKIPA Chair)	X		
NASA	X		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

Following the HEBCA Technical Testing vote, there was discussion in the meeting about whether the testing was done in the FPKI OA lab or at the HEBCA site at Dartmouth College. Until this issue could be resolved, a motion was made by NASA and seconded by DoD, to withdrawal approval of the HEBCA Technical Testing.

Here is the voting record:

Vote to withdrawal the approval of the HEBCA Technical Testing			
Voting members	**Vote (Motion – NASA; 2nd – DoD)**		
	Yes	**No**	**Abstain**
Dept of Commerce (designated proxy - FPKIPA Chair)	X		
Dept of Defense	X		
Dept of Energy	ABSENT – did not vote		
Dept of Health & Human Services	X		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury	ABSENT – did not vote		
GSA (designated proxy - FPKIPA Chair)	X		
NASA	X		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

While waiting for resolution of the location of the HEBCA technical testing, Mr. Brant Petrick, FICC, led the discussion of the Cybertrust CPS change. The only change that Cybertrust made to their CPS is designed to more accurately describe the policy Cybertrust follows in generating CRLs (i.e. issue CRLs every 12 hours with the validity period for the CRL set at 18 hours). Here is the voting record:

Approval vote for Cybertrust CPS Change			
Voting members	**Vote (Motion – State; 2nd – USPTO)**		
	Yes	**No**	**Abstain**
Dept of Commerce (designated proxy - FPKIPA Chair)	X		
Dept of Defense	X		
Dept of Energy	ABSENT – did not vote		
Dept of Health & Human Services	X		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury	ABSENT – did not vote		
GSA (designated proxy - FPKIPA Chair)	X		
NASA	X		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

The FPKI OA was able to validate and inform the FPKIPA that the final testing for HEBCA was done with the HEBCA system at Dartmouth College, so the FPKIPA agreed to vote again to approve the HEBCA Technical Testing. Here is the voting record:

Approval vote for HEBCA Technical Testing			
Voting members	**Vote (Motion – NASA; 2nd – NFC)**		
	Yes	**No**	**Abstain**
Dept of Commerce (designated proxy - FPKIPA Chair)	X		
Dept of Defense	X		
Dept of Energy	ABSENT – did not vote		
Dept of Health & Human Services	X		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury	ABSENT – did not vote		
GSA (designated proxy - FPKIPA Chair)	X		
NASA	X		
OMB	ABSENT – did not vote		

USDA/NFC	X		
USPTO	X		

Department of Homeland Security (DHS) – technical testing for DHS was completed on 11 February 2005. The testing was done with the Critical Path directory product, which DHS will use in their production PKI for the foreseeable future. However, the report also mentioned the possibility of DHS using the Siemens directory product in the future, once some of its current technical problems are resolved. The FPKIPA voting members wanted the report to not mention the potential use of the Siemens product before they voted to approve the DHS Technical Testing.

ACTION (127): The FPKI OA will update the DHS Technical Testing Report to delete references to potential future use of the Siemens directory product by DHS.

ACTION (128): IATAC will request an email vote for approval of DHS Technical Testing once it receives the updated report.

ACTION (129): If the DHS Technical Testing is approved, IATAC will request an email vote for approval of DHS for Cross-Certification at the Medium assurance level.

Status of CA Testing:
There was no CA testing since the 8 February FPKIPA meeting to report during this meeting.

Agenda Item 10

Final Meeting Items

State of Illinois Audit Extension
The State of Illinois has experienced delays in their normal audit cycles and thought they needed to seek an extension for their annual audit. However, since the FPKIPA received and approved their June 2004 audit by email vote on 4 March 2005, the FPKIPA isn't expecting the next audit from the State of Illinois until June 2005, so an audit extension is not necessary at this time.

Kickoff Meeting for National Security Bridge Working Group
Ms. Debbie Mitchell, DoD PKI PMO, announced that this will be a teleconference meeting and has been scheduled for 16 March from 09:00 a.m. – 11:00 a.m. The dial-in phone number will be 1-866-657-9756, passcode is 3020401.
So far, the expected participating organizations are DoD, DHS, Energy, Justice, NASA, State, and Treasury.

Department of State
The Department of State is transitioning their directory architecture to Microsoft Active Directory. With this change in the directory architecture, does State need to reapply for cross-certification? No, they just need to test the directory interoperability with the FPKI OA.

Also, State announced that as of this date, the DoD Common Access Card (CAC) is now recognized, using biometrics for authentication, in the State PKI.

Agenda Item 11

Meeting Adjourned / Next Meeting Plans
The meeting adjourned at 11:40 a.m.

The next FPKI PA Meeting is scheduled for 12 April 2005 from 09:30-12:30 at the GSA facility located at 1800 F Street, Room 2239, Washington, DC.

D. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	13 Jan 2004 FPKIPA meeting	**Open**
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
066	Develop text for the FPKIPA Charter regarding the sunset clause for voting members of the FPKIPA who are not cross certified members of the FBCA.	Tim Polk, NIST	18 Nov 2003	13 Jan 2003 FPKIPA meeting	**Open**
085	Test/evaluate the PKCS-12 usage issue and make a recommendation to the FPKIPA at a meeting in the near future.	Tim Polk, NIST	13 July 2004	12 October 2004 FPKIPA meeting	**Open**
087	Once the CPWG approves the Department of Labor (DoL) compliance audit letter, request the FPKIPA voting members to submit their approval votes for cross certification of DoL.	IATAC	13 July 2004	10 August 2004 FPKIPA meeting	**Open**
090	Develop a C&A list related to NIST Standards 800-26 and 800-53.	Cheryl Jenkins, GSA	12 Oct 2004	Jan 2005 FPKIPA meeting	**Open**
095	Develop, obtain FPKIPA approval, and distribute a letter to cross-certification members, requesting them to send a letter to the FPKIPA to document their compliance audit history and schedule of annual audit of their cross-certified CA, in compliance with FISMA requirements.	IATAC	12 Oct 2004	14 Dec 2004 FPKIPA meeting	**Open**
096	Research and draft FPKIPA charter updates to address Bridge-to-Bridge Cross-Certification.	Dr. Tice DeYoung, NASA	12 Oct 2004	Jan 2005 FPKIPA meeting	**Open**

No.	Action Statement	POC	Start Date	Target Date	Status
097	Research and draft FBCA Criteria & Methodology document updates to address Bridge-to-Bridge Cross-Certification.	Dr. Peter Alterman, HHS	12 Oct 2004	Jan 2005 FPKIPA meeting	**Open**
112	Update their MOA with the FBCA to reflect the new one-way certificate being issue for the period of January 2005 to January 2006.	DoD	11 Jan 2005	28 Feb 2005	**Open**
113	Prepare and route a new Letter of Authorization from the FPKIPA to the FPKI OA for this new one-way cross-certificate for the DoD PKI for the period of January 2005 to January 2006.	IATAC	11 Jan 2005	31 Jan 2005	**Open**
115	Develop a FPKIPA Business Practices document.	Dr.Tice DeYoung, NASA Charles Froehlich, State (Mantech)	11 Jan 2005	31 Mar 2005	**Open**
124	Develop a memo from the FPKIPA to the FBCA Cross-Certification members to request the maintenance of a long-term prototype CA at each of their sites.	Cheryl Jenkins, FPKI OA Director	08 Feb 2005	8 Mar 2005 FPKIPA meeting	**Open**
125	Coordinate a FBCA TWG meeting to be held in early March 2005, to discuss FBCA Directory problems identified by Treasury.	Cheryl Jenkins, FPKI OA Director	08 Feb 2005	4 Mar 2005	**Open**
126	Determine using the Entrust CA product, how soon it will be practical to transition to the use of SHA-256.	Cheryl Jenkins, FPKI OA Director	08 Mar 2005	12 April 2005 FPKIPA meeting	**Open**
127	Update the DHS Technical Testing Report to delete references to potential future use of the Siemens directory product by DHS.	FPKI OA	08 Mar 2005	09 Mar 2005	**Closed, 08 Mar 2005**
128	Request an email vote for approval of DHS Technical Testing, once it receives the updated report.	IATAC	08 Mar 2005	09 Mar 2005	**Closed, 09 Mar 2005**
129	If the DHS Technical Testing is approved, request an email vote for approval of DHS for Cross-Certification at the Medium assurance level.	IATAC	08 Mar 2005	14 Mar 2005	**Open**

Appendix A

FPKIPA Email Voting Record (8 Feb 2005 – 7 Mar 2005)

ORG	**PTO Approval of Compliance Audit and XCert (Med)** **Request –** **16 Feb 2005** **Due–** **23 Feb 2005** **Approval –** **23 Feb 2005**	**Voting Member**	**State of Illinois Compliance Audit (dated Sept 2004)** **Request –** **1 Mar 2005** **Due –** **4 Mar 2005** **Approval –** **4 Mar 2005**	**Voting Member**
Commerce	**Y 02/17/05**	**Polk**	**Y 03/02/05**	**Polk**
Defense	**Y 02/16/05**	**Hanko**	**Y 03/07/05**	**Mitchell**
Energy	**Y 02/17/05**	**Wujcik**	**Y 03/01/05**	**Bales**
HHS	**Y 02/16/05**	**Alterman**	**Y 03/01/05**	**Alterman**
Justice	**Y 02/16/05**	**Deeley**	**Y 03/02/05**	**Deeley**
State	**Y 02/22/05**	**Cao**	**Y 03/02/05**	**Cao**
Treasury	**Y 03/03/05**	**Schminky**	**Y 03/02/05**	**Schminky**
GSA	**Y 02/23/05**	**Temoshok**	**Y 03/02/05**	**Temoshok**
NASA	**Y 02/17/05**	**DeYoung**	**Y 03/02/05**	**DeYoung**
OMB	**Y 03/07/05**	**Thornton**	**Y 03/02/05**	**Thornton**
USDA/NFC	**Y 02/22/05**	**Sharp**	**Y 03/01/05**	**Sharp**
	Result – Approved Y – 11 of 11 votes (100%)		**Result – Approved** Y – 11 of 11 votes (100%)	